

RECEIVED
CENTRAL FAX CENTER**MAR 31 2005****Yee &
Associates, P.C.**4100 Alpha Road
Suite 1100
Dallas, Texas 75244Main No. (972) 385-8777
Facsimile (972) 385-7766**Facsimile Cover Sheet**

To: Commissioner for Patents for Examiner Brandon S. Hoffman Group Art Unit 2136	Facsimile No.: 703/872-9306
From: Amelia Turner Legal Assistant to Lisa L.B. Yociss	No. of Pages Including Cover Sheet: 27
Message: Transmitted herewith: <ul style="list-style-type: none">• Transmittal Document; and• Appeal Brief.	
Re: Application No.: 09/687,100 Attorney Docket No: AUS9-2000-0401-US1	
Date: Thursday, March 31, 2005	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-385-7766.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gusler et al.

Serial No.: 09/687,100

Filed: October 12, 2000

For: Method and System for Building
Dynamic Firewall Rules, Based on
Content of Downloaded Documents

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER§
§
§
§
§
§

Group Art Unit: 2136

Examiner: Hoffman, Brandon S.

Attorney Docket No.: AUS9-2000-0401-US1

Certificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306, on March 31, 2005.

By:

Amelia C. Turner

TRANSMITTAL DOCUMENTCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

TRANSMITTED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of \$500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,


Catherine K. Kinslow

Registration No. 51,886

Duke W. Yee

Registration No. 34,285

YEE & ASSOCIATES, P.C.

P.O. Box 802333

Dallas, Texas 75380

(972) 385-8777

ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

MAR 31 2005

Docket No. AUS9-2000-0401-US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gusler et al.

§

Serial No. 09/687,100

§

Group Art Unit: 2136

§

Filed: October 12, 2000

§

Examiner: Hoffman, Brandon S.

§

For: Method and System for Building
Dynamic Firewall Rules, Based on
Content of Downloaded Documents

§

§

§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (703) 872-9306,
on March 31, 2005.

By:

Amelia C. Turner
Amelia C. Turner

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on January 31, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this
brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL
BRIEF.

(Appeal Brief Page 1 of 25)
Gusler et al. - 09/687,100

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation, as reflected in the Assignment recorded on October 12, 2000, at Reel 011279, Frame 0659.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1, 3-8, and 10-15.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 2 and 9.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1, 3-8, and 10-15.
4. Claims allowed: None.
5. Claims rejected: 1, 3-8, and 10-15.
6. Claims objected to: None.

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-8, and 10-15.

STATUS OF AMENDMENTS

There are no amendments after the Final Rejection that was mailed December 9, 2004.

SUMMARY OF CLAIMED SUBJECT MATTER

Applicants' independent claim 1 describes a method for filtering incoming data from an external computer network. (Specification page 4, lines 2-4.) A firewall is coupled to the external computer network. A server computer system is coupled to an internal computer network. A plurality of clients are coupled to the server computer system. (Figure 1, and specification page 6, lines 5-10.) The plurality of clients are unable to access the external computer network directly. (Figure 1, and specification page 6, lines 5-10.) A document is received at the firewall from the external computer network. (Specification page 7, lines 23-26.) The firewall determines whether the document is from a known blocked site. (Specification page 7, lines 26-29.) In response to determining that the document is from a known blocked site, the firewall blocks the document without scanning the document. (Specification page 8, lines 28-32.) The firewall determines whether the document is from a known safe site. (Specification page 8, lines 2-4.) In response to determining that the document is from a known safe site, the firewall forwards the document to the server without scanning the document. (Specification page 8, lines 8-11.) All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 5-10, Figure 1, and specification page 9, lines 16-18.) In response to determining that the document is not from a known blocked site or a known safe site, the firewall scans text fields included in the document for pre-selected keyword(s). (Specification page 8, lines 12-23.) The firewall blocks the document if any of the text fields include content that contains pre-selected keywords. (Specification page 8, lines 24-32.) The server computer system is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 5-10, Figure 1, specification page 7, line 31 through page 8, line 1, and specification page 8, lines 24-32.) The firewall indicates that a site that sent the document is a known blocked site by adding the address of the site to a filtering table. (Specification page 8, lines 24-32.)

Applicants' claim 6 depends on claim 1 and describes the addition of a site to the filtering table being implemented using a strong text parsing language. (Specification page 8, line 32 through page 9, line 2.)

Applicants' claim 7 depends on claim 1 and describes the instance of the filter being periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables. (Specification page 9, lines 11-15.)

Applicants' independent claim 8 describes a computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network. (Specification page 4, lines 2-4.) A firewall is coupled to the external computer network. A server computer system is coupled to an internal computer network. A plurality of clients are coupled to the server computer system. (Specification page 6, lines 5-10 and Figure 1.) The plurality of clients are unable to access the external computer network directly. (Specification page 6, lines 5-10 and Figure 1.) The product includes instructions for receiving at the firewall a document from the external computer network. (Specification page 7, lines 23-26.) Instructions are included for determining, by the firewall, whether the document is from a known blocked site. (Specification page 7, lines 26-29.) In response to determining that the document is from a known blocked site, instructions are included for blocking the document without scanning the document. (Specification page 8, lines 28-32.) Instructions are included for determining, by the firewall, whether the document is from a known safe site. (Specification page 8 lines 2-4.) In response to determining that the document is from a known safe site, instructions are included for forwarding the document to the server without scanning the document. (Specification page 8, lines 8-11.) All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 5-10, Figure 1, and specification page 9, lines 16-18.) In response to determining that the document is not from a known blocked site or a known safe site, instructions are included for scanning, by the firewall, text fields included in the document for pre-selected keyword(s). (Specification page 8, lines 12-23.) Instructions are included for blocking, by the firewall, the document if any of the text fields include content that contains pre-selected keywords. (Specification page 8, lines 24-32.) The server computer system is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 5-10, Figure 1, specification page 7, line 31 through page 8, line 1, and specification page 8, lines 24-32.) Instructions are included for indicating that a site that sent the document is a known blocked site by adding, by the firewall, the address of the site to a filtering table. (Specification page 8, lines 24-32.)

Applicants' claim 13 depends on claim 8 and describes the instructions for addition of a site to the filtering table being implemented in a strong text parsing language. (Specification page 8, line 32 through page 9, line 2.)

Applicants' claim 14 depends on claim 8 and describes the instance of the filter being periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables. (Specification page 9, lines 11-15.)

Applicants' independent claim 15 describes a system for filtering incoming data from an external computer network. (Specification page 4, lines 2-4.) A firewall is coupled to the external computer network. A server computer system is coupled to an internal computer network. A plurality of clients are coupled to the server computer system. (Specification page 6, lines 5-10.) The plurality of clients are unable to access the external computer network directly. (Specification page 6, lines 5-10 and Figure 1.) The firewall is for receiving a document from the external computer network. (Specification page 7, lines 23-26.) The firewall is for determining whether the document is from a known blocked site. (Specification page 7, lines 26-29.) In response to determining that the document is from a known blocked site, the firewall is for blocking the document without scanning the document. (Specification page 8, lines 28-32.) The firewall is for determining whether the document is from a known safe site. (Specification page 8, lines 2-4.) In response to determining that the document is from a known safe site, the firewall is for forwarding the document to the server without scanning the document. (Specification page 8, lines 8-11.) All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 5-10, Figure 1, and specification page 9, lines 16-18.) In response to determining that the document is not from a known blocked site or a known safe site, the firewall is for scanning text fields included in the document for pre-selected keyword(s). (Specification page 8, lines 12-23.) The firewall is for blocking the document if any of the text fields include content that contains pre-selected keywords. (Specification page 8, lines 24-32.) The server computer system is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 5-10, Figure 1, specification page 7, line 31 through page 8, line 1, and specification page 8, lines 24-32.) The firewall is for indicating that a site that sent the document is a known blocked site by adding the address of the site to a filtering table. (Specification page 8, lines 24-32.)

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1, 3-8, and 10-15)

Claims 1, 3-8, and 10-15 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*.

B. GROUND OF REJECTION 2 (Claims 6 and 13)

Claims 6 and 13 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*, and further in view of U.S. Patent 6,662,241 issued to *Bauer*.

C. GROUND OF REJECTION 3 (Claims 7 and 14)

Claims 7 and 14 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*, and further in view of *Webopedia* (<http://www.webopedia.com/TERM/C/cron.html>).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1, 3-8, and 10-15)

Claims 1, 3-8, and 10-15 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*. This position is not well founded.

Applicants claim a firewall that is coupled to an external computer network, and a server computer system that is coupled to an internal computer network. A plurality of clients are coupled to the server where the clients are unable to access the external computer network directly. The firewall receives a document and determines whether it is from a known blocked site. If the firewall determines that the document is from a known blocked site, the firewall blocks the document without scanning it. The firewall determines whether the document is from a known safe site. If the document is from a known safe site, the firewall forwards the document to the server without scanning it. All of the clients are permitted to access the forwarded document.

If the firewall determines that the document is not from a known safe site or known blocked site, the firewall scans text fields in the document for pre-selected keywords. The firewall blocks the document if any of the text fields include content that contains pre-selected keywords. The server is prohibited from receiving the document if the document is blocked. The firewall indicates that a site that sent the document is a known blocked site by adding the address of the site to a filtering table.

The Examiner relies on *Baker* for teaching most of the features of the claims. The Examiner states that *Baker* teaches all of the features except for the firewall scanning text fields in the document for pre-selected keywords, the firewall blocking the document if any of the text fields include content that contains pre-selected keywords, or the firewall indicating that a site that sent the document is a known blocked site by adding the address of the site to a filtering table. The Examiner relies on *Hughes* to supply the features believed missing from *Baker*.

Applicants disagree with the Examiner that *Baker* teaches the remaining features of the claims. *Baker* teaches user terminals that are coupled to a proxy server that is coupled to a firewall that is coupled to a public network. The firewall of *Baker* does not function in the manner claimed by Applicants.

Baker teaches rating information and then using these ratings to restrict specific users from being able to access the information. A request is made from one of the user terminals 107-109 to access a public network 100. The request is in the form of a URL. Thus, a particular URL is requested from one of the user terminals 107-109. This requested URL is submitted to a proxy server 112. The proxy server 112 then determines the identity of the particular user terminal that made the request.

The proxy server 112 includes a database 114 that includes a user clearance for each user terminal and a list of allowable URLs. The user clearance indicates a particular rating class that the user is allowed to access. In addition, the list of allowable URLs associates each URL with a particular resource rating. When a particular user terminal attempts to access a particular allowable URL, the proxy server 112 compares the user terminal's user clearance to the resource rating assigned to the requested URL. If that particular user terminal has clearance to access URLs having the resource rating that is associated with the requested URL, the proxy server 112 forwards the requested URL to the public network 100 via the firewall 113. Thus, the particular user terminal is permitted to access the requested URL. The public network 100 then returns the requested information to the user terminal via the firewall 113 and proxy server 112. Otherwise, if the particular user terminal does not have clearance to access a URL having the resource rating associated with the requested URL, the proxy server 112 denies the request to access the requested URL and the proxy server 112 does not send the requested URL to the public network 100.

Applicants claim a firewall that is coupled to an external computer network. The Examiner states that *Baker* teaches a firewall that is coupled to an external computer network at figure 1, reference number 113. Firewall 113 is coupled to a public network 100.

Applicants claim a server that is coupled to an internal computer network. The Examiner states that *Baker* teaches a server that is coupled to an internal computer network at figure 1, reference number 112. *Baker* refers to the block referenced as 112 as a proxy server 112. Proxy server 112 is coupled to firewall 113.

Applicants claim a plurality of clients that are coupled to the server where the clients are unable to access the external network computer network directly. The Examiner states that *Baker* teaches this feature at figure 1, reference numbers 107-109. *Baker* refers to the blocks referenced as 107-109 as user terminals 107-109. User terminals 107-109 are coupled to the proxy server 112.

Applicants claim a document being received at the firewall from the external network. The Examiner states that *Baker* teaches this feature at column 6, lines 8-12. Column 6, lines 8-12, describes processor 111 receiving an incoming URL. Processor 111 then determines the identity of the user terminal from the URL header and uses the identification to determine the clearance category specification for that user.

The cited section of *Baker* does not teach Applicants' claimed feature because the cited section does not teach the action of receiving a document and does not teach a firewall performing an action.

The cited section of *Baker* does not teach a document being received by the firewall from the external network. The cited section teaches a request for a URL being received by the proxy server. A request for a URL is not a document.

The cited section of *Baker* makes is clear that it is proxy server 112 that receives the request for a document, and not the firewall.

Baker does teach the firewall receiving the page associated with the requested URL in other sections of *Baker*. A user terminal requests a document by transmitting a requested URL to the proxy server. If the user terminal is approved for receiving the type of information that is associated with the requested URL, the proxy server will transmit the requested URL to the public network via the firewall. At that time, the public network will return the page associated with the requested URL to the proxy server via the firewall. However, for the reasons described below, *Baker*, in combination with *Hughes*, does not render Applicants' claims unpatentable because the firewall of *Baker* does not behave in a manner such as claimed by Applicants.

Applicants claim the firewall receiving a document and then making determinations about whether to block, forward, or scan the document. In *Baker*, the user terminal requests a document by requesting a URL. In *Baker*, this request is made to the proxy server, not the firewall. If the user terminal is approved for receiving the requested type of document, the proxy server will transmit the requested URL to the public network via the firewall. At that time the requested document is transmitted from the public network to the proxy server through the firewall. Thus, in *Baker*, a determination is made before the document is ever received as to whether the document should be received by the proxy server. According to Applicants' claims, a document is first received by the firewall and then a determination is made as to whether to block, forward, or scan

the document. In *Baker*, a determination of whether to receive the document is made before transmitting a request for the document. Thus, in *Baker*, a determination is made before the document is ever received.

Further, the firewall of *Baker* does not make any determination at all about the requested URL or the page associated with the URL was requested. The firewall of *Baker* merely forwards URLs that are requested by the proxy server to the public network and then sends the page associated with the URL back to the proxy server. It is the proxy server, not the firewall, that makes a determination as to whether to transmit the URL request.

Applicants claim the firewall determining whether the document is from a known blocked site. The Examiner states that *Baker* teaches this feature at column 6, lines 20-23. The cited section of *Baker* teaches the processor 111, within proxy server 112, denying the request if the requested URL is associated with a resource rating for which the requesting user terminal is not cleared. The cited section does not teach the firewall determining whether the document is from a known blocked site.

Applicants claim the firewall blocking the document if it is from a known blocked site. The Examiner again refers to *Baker* at column 6, lines 20-23. This section of *Baker* teaches that it is the processor in the proxy server, and not the firewall, that blocks the document. If the processor in the proxy server determines that the user is not approved for the requested URL, the proxy server does not send the URL to the firewall. Therefore, in cases where the proxy server determines that the user is not approved for the requested URL, the firewall never sees the requested URL.

Applicants claim the firewall determining if the document is from a known safe site. The Examiner refers to *Baker* at column 6, lines 13-20. This section of *Baker* describes the processor 111 of the proxy server 112 checking a listing to determine the resource rating of the requested URL. If the user terminal has clearance for the type of resource rating which is associated with the requested URL, the processor 111 of the proxy server 112 forwards the requested URL to the public network 100 through the firewall 113. Thus, the cited section of *Baker* does not teach a firewall making a determination.

Applicants claim the firewall forwarding the document to the server without scanning the document if a determination is made that the document is from a known safe site. Further, Applicants' claim all of the clients being permitted to access the forwarded document. The

Examiner refers to *Baker* at column 6, lines 13-20 as teaching these features. This section of *Baker* teaches the processor of the proxy server, not the firewall, performing the actions described in the cited section.

Further, *Baker* does not teach making a document available to all of the user terminals. *Baker* teaches tailoring the permissions to access particular kinds of documents to each user terminal. It would defeat the purpose of *Baker* to forward a document that was requested by one user terminal having one set of permissions to all user terminals that may have different sets of permissions.

Further, *Baker* does not teach scanning the document. Regarding other features, the Examiner states that *Baker* does not teach scanning text fields and uses *Hughes* to supply these features that are missing from *Baker*. However, the Examiner appears to believe that *Baker* teaches forwarding without scanning. *Baker* provides no teaching about forwarding without scanning if the document is from a known safe site.

Applicants claim the server being prohibited from receiving the document if the document is from a blocked site. The Examiner again refers to *Baker* at column 6, lines 20-23. *Baker* does not teach a server being prohibited from receiving the document if the document is from a blocked site. In *Baker*, it is the proxy server that determines whether or not to transmit a requested URL to the public network. If the proxy server determines that the URL should be transmitted, the proxy server transmits the URL and then receives the page associated with that URL. If the proxy server determines that the URL should not be transmitted, the proxy server does not transmit the URL. The proxy server is not prohibited from receiving a document if the document is from a known blocked site. The proxy server is the device that makes the decision as to whether to transmit a URL. The proxy server is not prohibited from transmitting a particular URL, it decides not to.

The Examiner states that *Baker* does not teach the firewall scanning text fields for keywords if the document is not from a known blocked or known safe site. The Examiner relies on *Hughes* to supply the features believed missing from *Baker*. The combination of *Baker* and *Hughes*, however, does not teach the firewall scanning text fields for keywords if the document is not from a known blocked or known safe site. *Hughes* teaches scanning local memory to determine whether inappropriate content is present.

Placing a scanning process into the firewall of *Baker* does not render Applicants' claims unpatentable because the combination does not teach the other features of Applicants' claims. Having the firewall of *Baker* scan the page that was associated with a requested URL does not teach the combination of the other features of Applicants' claims.

The firewall of *Baker* does not perform the other features of the claims being performed as claimed by Applicants. As discussed above, the firewall of *Baker* does not first receive a document from the external network, then determine whether the document is from a known blocked or known safe site, block the document if it is from a known blocked site without scanning the document, or forward the document to the server without scanning it if it is from a known safe site where all of the clients can access the forwarded document.

The combination of *Baker* and *Hughes* would result in a firewall that scans received pages but does not first receive a document from the external network, then determine whether the document is from a known blocked or known safe site, block the document if it is from a known blocked site without scanning the document, or forward the document to the server without scanning it if it is from a known safe site where all of the clients can access the forwarded document.

The Examiner also states that *Baker* does not teach blocking the document if it includes content that contains pre-selected keyword and relies on *Hughes* to supply this feature. As described above, the combination of *Baker* and *Hughes* does not teach this feature because the combination does not teach the other features of the claims being performed as claimed by Applicants.

The Examiner states that *Baker* does not teach the firewall indicating that a site that sent the document is a known blocked site by adding the site to a filtering table. The Examiner again relies on *Hughes* to supply this missing feature. Again, the combination of *Baker* and *Hughes* does not teach this feature because the combination does not teach the other features of the claims being performed as claimed by Applicants.

The combination of *Baker* and *Hughes* does not render Applicants claims unpatentable because the combination does not teach the particular combination of firewall, server, and client computer systems. The combination does not teach a firewall performing the steps as claimed by Applicants.

B. GROUND OF REJECTION 2 (Claims 6 and 13)

Claims 6 and 13 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*, and further in view of U.S. Patent 6,662,241 issued to *Bauer*. This position is not well founded.

Applicants' claims 6 and 13 describe the addition of a site to the filtering table being implemented using a strong text parsing language. The Examiner states that the combination of *Baker* and *Hughes* does not teach this feature and relies on *Bauer* to supply the missing feature.

Specifically, the Examiner refers to column 1, lines 11-25 of *Bauer*. This section of *Bauer* teaches a scripting language, such as Perl, that provides strong file and text manipulation.

The combination of *Baker*, *Hughes*, and *Bauer* does not teach the combination of the addition of a site to the filtering table being implemented using a strong text parsing language in combination with the other features of the claims because the combination of *Baker* and *Hughes* does not teach the particular claimed combination of firewall, server, and client computer systems where the firewall performs the steps as claimed by Applicants.

C. GROUND OF REJECTION 3 (Claims 7 and 14)

Claims 7 and 14 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 5,678,041 issued to *Baker* in view of U.S. Patent 6,389,472 issued to *Hughes*, and further in view of *Webopedia* (<http://www.webopedia.com/TERM/C/cron.html>). This position is not well founded.

Applicants' claims 7 and 14 describe the instance of the filter being periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables. The Examiner states that the combination of *Baker* and *Hughes* does not teach this feature and relies on *Webopedia* to supply the missing feature.

The combination of *Baker*, *Hughes*, and *Webopedia* does not teach the combination of the instance of the filter being periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables in combination with the other features of the claims because the combination of *Baker* and *Hughes* does not teach the particular claimed combination of firewall, server, and client computer systems where the firewall performs the steps as claimed by Applicants.

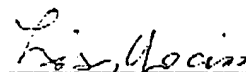
D. CONCLUSION

The combination of *Baker* and *Hughes* does not render Applicants' claims unpatentable because the combination does not describe, teach, or suggest the particular combination of firewall, server, and client computer systems where the firewall performs the steps as claimed by Applicants.

The combination of *Baker*, *Hughes*, and *Bauer* does not render Applicants' claims unpatentable because the combination does not describe, teach, or suggest the combination of the addition of a site to the filtering table being implemented using a strong text parsing language in combination with the other features of the claims because the combination of *Baker* and *Hughes* does not teach the particular claimed combination of firewall, server, and client computer systems where the firewall performs the steps as claimed by Applicants.

The combination of *Baker*, *Hughes*, and *Webopedia* does not render Applicants' claims unpatentable because the combination does not describe, teach, or suggest the combination of the instance of the filter being periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables in combination with the other features of the claims because the combination of *Baker* and *Hughes* does not teach the particular claimed combination of firewall, server, and client computer systems where the firewall performs the steps as claimed by Applicants.

Therefore, Applicants' claims are believed to be patentable over the cited prior art.



Lisa L.B. Tociss
Reg. No. 36,975
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal reads:

1. A method for filtering incoming data from an external computer network, comprising:
a firewall that is coupled to said external computer network;
a server computer system coupled to an internal computer network;
a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;
receiving, at said firewall, a document from said external computer network;
determining, by said firewall, whether said document is from a known blocked site;
in response to determining that said document is from a known blocked site, blocking, by said firewall, said document without scanning said document;
determining, by said firewall, whether said document is from a known safe site;
in response to determining that said document is from a known safe site, forwarding, by said firewall, said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;
in response to determining that said document is not from a known blocked site or a known safe site, scanning, by said firewall, text fields included in said document for pre-selected keyword(s);
blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;
said server computer system being prohibited from receiving said document in response to said document being blocked; and

indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

3. The method according to claim 1, wherein the document is allowed to pass per standard service rules if the content does not contain pre-selected keyword(s).
4. The method according to claim 1, further comprising storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.
5. The method according to claim 1, wherein the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table further comprises adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.
6. The method according to claim 1, wherein the addition of a site to the filtering table is implemented using a strong text parsing language.
7. The method according to claim 1, wherein the instance of the filter is periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables.

8. A computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network, the computer program product comprising:

a firewall that is coupled to said external computer network;

a server computer system coupled to an internal computer network;

a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;

instructions for receiving, at said firewall, a document from said external computer network;

instructions for determining, by said firewall, whether said document is from a known blocked site;

in response to determining that said document is from a known blocked site, instructions for blocking said document without scanning said document;

instructions for determining, by said firewall, whether said document is from a known safe site;

in response to determining that said document is from a known safe site, instructions for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, instructions for scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

instructions for blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and

instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

10. The computer program product according to claim 8, further comprising instructions for allowing the document to pass per standard service rules if the content does not contain pre-selected keyword(s).

11. The computer program product according to claim 8, further comprising instructions for storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.

12. The computer program product according to claim 8, wherein the instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, that address of said site to a filtering table further comprises adding the address of said site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

13. The computer program product according to claim 8, wherein the instructions for addition of a site to the filtering table are implemented in a strong text parsing language.

14. The computer program product according to claim 8, wherein the instance of the filter is periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables.

15. A system for filtering incoming data from an external computer network, the system comprising:

- a firewall that is coupled to said external computer network;
- a server computer system coupled to an internal computer network;
- a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;
- said firewall for receiving a document from said external computer network;
- said firewall for determining whether said document is from a known blocked site;
- in response to determining that said document is from a known blocked site, said firewall for blocking said document without scanning said document;
- said firewall for determining whether said document is from a known safe site;
- in response to determining that said document is from a known safe site, said firewall for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;
- in response to determining that said document is not from a known blocked site or a known safe site, said firewall for scanning text fields included in said document for pre-selected keyword(s);
- said firewall for blocking the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and

said firewall for indicating that a site that sent said document is a known blocked site by adding the address of said site to a filtering table.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.